

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

REMARKS

This Amendment is in response to the Office Action mailed 10/21/2004. Reconsideration in light of the remarks made herein is respectfully requested.

This Amendment is in response to the Final Office Action mailed 10/21/2004. Applicant has filed a Request for Continued Examination to have the Office withdraw the finality of the Office Action and have this submission entered and considered. In the Office Action, the Examiner rejected claims 1-5 and 11-46 under 35 U.S.C. § 102, and rejected claims 6-10 under 35 U.S.C. § 103. No claims are amended. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Examiner's Response to Arguments

The Examiner considered applicant's arguments filed 9/20/2004 and found them unpersuasive. Applicant respectfully requests that the Examiner reconsider applicant's arguments in light of the additional remarks below.

The Examiner understands applicant's previous remarks to indicate that applicant understands Arrow to be only for configuring VPN units for use on a VPN prior to creation of the VPN via the public network. The Examiner misunderstands the intent of applicant's remark regarding configuration prior to the creation of the VPN. Arrow discloses the one of the capabilities of the VPN Management Station is to direct boot loading and initial configuration of a VPN unit in columns 9 through 10. Applicant presents this as evidence that Arrow discloses a VPN Management Station that is capable of communicating with a VPN unit before a VPN is

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

configured and therefore evidence that the VPN Management Station does not communicate with the VPN Unit using a VPN.

The Examiner provides a thorough review of Arrow that stresses that a VPN may be built on top of a public network. Applicant agrees that VPNs are built using an OSI Layer 2 Tunneling Protocol that allows a secured virtual network to be built on an unsecured physical network. The Examiner states that "the VPN units are part of the VPN, as is the management station." To avoid any possible misunderstanding, applicant points out that the VPN does not exist in any physical form and it is not really clear what it means to say that a physical device, such as the VPN units or the management station, are part of the VPN. Applicant understands the VPN units to implement a VPN by serving as a bridge between a secured network and an unsecured network by encapsulating messages received from the secured network for transit through the unsecured network, and unencapsulating messages received from the unsecured network and returning them to the secured network. The significance of this is that the VPN units must be able to communicate with both the secured and the unsecured networks to be able to create the VPN by translating and passing messages between the two networks. Applicant respectfully submits that no inference can be drawn that communication with a VPN unit is carried out over a VPN simply because the VPN unit is capable of implementing a VPN.

Both the Examiner and the applicant point to Arrow's disclosure that, "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100" at col. 6, lines 31-34, to support their opposite conclusions. The Examiner concludes that this statement indicates that the communication between the management station and the VPN units is over the

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

VPN built on the public network. The applicant considers this statement to indicate that communication between the management station and the VPN units is over the public network without the use of a VPN.

The Examiner especially notes that if the source and destination address for the data packet are not members of the same VPN, then the packet is forwarded to the Internet as ordinary Internet traffic, as though the VPN unit were not involved. The Examiner points to this as clear evidence that packets sent between VPN units are carried over the VPN, otherwise the traffic is considered to be ordinary Internet traffic. Applicant respectfully submits that this is an unremarkable observation. The purpose of a VPN is to replace a segment of a secured network with an unsecured network. Therefore traffic between VPN units, which is the traffic on the unsecured network, must be carried on the VPN that is by definition the surrogate for the portion of the secured network that is actually carried on an unsecured network. It is likewise unremarkable that data packets between a source and a destination address that are not members of the same VPN is treated as ordinary Internet traffic. To say that they are not members of the same VPN is to say that the source and destination addresses are in different secured networks; there is no logical connection between the two networks of the source and destination. The fact that both secured networks might each use a VPN and that the two VPNs might be built on the same unsecured network is meaningless as regards the routing of data between the two networks. The only way to route data between the two secured, and therefore logically isolated, networks is by forwarding the data through an intermediary network connected to both secured networks, which the unsecured network must of necessity be to be able to provide a VPN for each of the two secured networks. Applicant respectfully submits that the more meaningful observation to

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

make regarding the passage in Arrow pointed to by the Examiner is that the VPN units are capable of dealing with both VPN traffic and ordinary Internet traffic.

The Examiner observes that column 10, lines 41-51 explicitly state that the VPN unit 115 is configured or reconfigured by VPN management station 160, so as to ensure that VPN unit 115 continues to operate during the configuration or reconfiguration. Applicant respectfully points out that the examples of the data essential to continued operation of the VPN unit given are the IP address of the VPN unit and the default route for communicating with the VPN management station. These items are necessary to permit ordinary Internet communication and are insufficient to define a VPN. Applicant respectfully submits that this is further evidence that the communication between the management station and the VPN unit is by means of ordinary Internet communication rather than over a VPN.

The Examiner points out that "configuring a VPN" includes editing or deleting an existing VPN. The Examiner then concludes that this requires that any information transferred between VPN units and the management station be transferred over the VPN itself, as non-VPN traffic is regarded and treated as regular Internet traffic and routed accordingly. Applicant respectfully submits that this is a faulty conclusion. The Examiner overlooks that the description of the routing of VPN traffic relates to traffic that has a destination address on a secured network. Management traffic will have a destination address of the VPN unit itself. The handling of traffic that passes through the VPN unit does not determine how traffic directed to the VPN unit will be handled.

The Examiner cites the disclosure by Arrow at col.15, lines 9-10, "A VPN unit object is created for each VPN unit in the network." The Examiner then appends the assertion, "the

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

network meaning the virtual private network." Applicant respectfully disagrees with this assertion. The VPN units are physical units in the physical unsecured Internet network that are capable of building numerous VPNs on the physical network. The only network that is assured of including all the VPN units that the management station would manage is the physical network. The VPNs are dynamic and numerous. A given VPN might have as few as two VPN units on the virtual private network. It is much more reasonable to assume that the network referred to in lines 9-10 is the physical network and not the virtual private network as the Examiner asserts.

The applicant's understanding that lines 9-10 refer to the physical network is further supported by lines 12-16 that disclose a group object is created for groups of network nodes on the public network. A group object includes an attribute identifying the VPN unit(s) associated with the group. In lines 16-23 Arrow discloses that a VPN object is created for each virtual private network supported by the VPN management station. A VPN object includes a list of groups. This clearly shows that a VPN management station may support more than one virtual private network. Further, the object hierarchy shows that the management station defines VPNs in terms of the groups included in the VPN and the groups define the VPN units included in any particular VPN. VPNs clearly do not define "each VPN unit in the network."

Considering the flow charts of Figures 13 and 14 for creating a VPN and a group, the Examiner asserts, "As the VPN itself is built over the public network 100 and communications between VPN units is via the VPN built over the network, it is clear that any communication between VPN units and the management station be carried over the VPN itself." Applicant respectfully disagrees with this logic. First, neither of the predicates--the VPN is built over the

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

public network nor communications between VPN units is via the VPN--involves the management station, therefore no conclusion about communication involving the management station can properly be reached. Second, the unconditional predicate that communications between VPN units is via the VPN is wrong because, as pointed out earlier by the Examiner, if the source and destination address for the data packet are not members of the same VPN, then the packet is forwarded to the Internet as ordinary Internet traffic, as though the VPN unit were not involved. Thus communications between VPN units is via the VPN only if the source and destination addresses are members of the same VPN. Finally, the Examiner fails to consider how the first group and the first VPN would be created if the management station communicated with VPN units over a VPN.

The Examiner concludes the review of Arrow by stating that the management or configuration of existing VPN units by the management station clearly requires the use of the VPN over the public network and that to conclude otherwise simply is not a proper reading of the Arrow reference in its entirety. Applicant respectfully disagrees. As applicant has pointed out above, the Examiner has made numerous unwarranted extrapolations from the disclosure of Arrow and injected unwarranted conclusions without distinguishing them from what is actually disclosed by Arrow. Applicant respectfully requests that the Examiner reconsider carefully what is disclosed by Arrow and what can and cannot be ascertained from the disclosure of Arrow regarding how communication between the management station and the VPN units is implemented.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Rejection Under 35 U.S.C. § 102

2. The Examiner rejects claims 1-5, 11-15, 16-21, 22-31, 32-41, and 42-46 under 35 U.S.C. § 102(e) as being anticipated by Arrow et al. (6,175,917).

Per claim 1, the Examiner asserts that a clear showing has been made that Arrow discloses the configuration of an existing VPN unit by the management station requires that the traffic be carried over the VPN because non-VPN traffic is treated as regular traffic and routed accordingly. Applicant respectfully submits that the Examiner's showing is far from clear and that Arrow more clearly shows that the configuration of an existing VPN unit by the management station requires that the traffic not be carried over the VPN and instead be carried as part of the normal public network traffic because the management station must be capable of communicating with an existing VPN unit to configure the first VPN.

Per claim 2, the Examiner asks, "How can the management station of a VPN not be part of the VPN, when only VPN traffic is allowed to travel over the VPN itself?" The management station does not participate in the transport of packets on the VPN and quite clearly the management station is not part of any VPN because, as seen in Figure 1, the management station is not connected to any LAN (secured network).

Per claim 3, applicant is persuaded by the Examiner argument that an interface to the public network is required in order to realize the VPN over the public network. Figure 4 shows a network communication port 414 connected to the public network 100. Applicant agrees that the network communication port 414 shown by Arrow is a management port since that is the only communication shown between the management station and the VPN unit in Figure 1. Arrow

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

discloses that a VPN unit forward or discard traffic is not being passed between members of the same VPN. Col. 7, lines 26-45. Thus Arrow clearly shows that the network communication port 414 is not limited to VPN traffic and nothing in Arrow discloses that the communication between the management station and the VPN unit, which is not traffic being routed through the VPN unit, is carried on a VPN.

Per claim 4, the Examiner asserts that Arrow discloses a management function (i.e. Figures 5 and 6) internal to 115 is linked with the VPN via the schematic of Figure 4. Applicant respectfully disagrees. Figure 4 shows a network communication port 414 connected to the public network 100. Applicant submits that nothing in Arrow discloses that the management function internal to the network device is linked with the VPN as claimed.

Per claim 5, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 11, the Examiner asserts that the method steps are met by configuring VPN unit 115 to support a VPN via section 160 and linking a management device 160 and its function with the VPN. Applicant respectfully disagrees. Applicant is unable to find anything in Arrow to support the inference that a management device and its function are linked with the VPN. As disclosed in column 9, the management device 160 of Arrow may be used to boot load the VPN unit 115 and to configure the unit. One skilled in the art would reasonably infer that the VPN management station 160 does not send management traffic over the VPN because the management station provides commands for establishing a virtual private network that operates over a public network. If the VPN management station 160 is used to establish a virtual private

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

network, the VPN management station cannot communicate with the VPN units to establish the VPN using the VPN that is not yet established. Applicant does not intend to say that Arrow is limited to establishing a VPN when no VPN yet exists, merely that Arrow does disclose that it is possible to do so. Clearly the VPN established when no VPN yet exists must be done with management traffic that is not carried on a VPN. Thus Arrow discloses that communication between the management station and a VPN unit can be over the public network with the use of a VPN. Nothing in Arrow discloses that communication between the management station and a VPN unit is handled differently once a VPN is established.

Per claim 12, the Examiner asserts that Arrow discloses the management traffic is carried over the VPN itself. As discussed above in connection with claim 11, the management device would be unable to communicate with VPN units to establish a VPN before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 13, the Examiner asserts that Arrow discloses the network device 115 is managed using the VPN carried management traffic. As discussed above in connection with claim 11, the network device could not be managed using VPN carried management traffic before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 14, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Per claim 15, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 16, the Examiner asserts that the VPN unit 115 is configured to support a VPN with a link that links a management function with the VPN via port 414. As discussed above in connection with claim 11, the management function would be unable to communicate with VPN units to establish a VPN before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 17, the Examiner asserts that Arrow discloses the routing and forwarding module delivers management traffic on the VPN for the network device 115. As discussed above in connection with claim 11, the management traffic would be unable to establish a VPN on the network device before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 18, as discussed above in connection with claim 11, the network device could not be managed using VPN carried management traffic before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 19, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Per claim 20, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 21, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 22, the Examiner asserts that the "means+function" are met by the means for receiving management traffic over the VPN, at for example, 414 and that the means for managing the network device using the management traffic received over the VPN is met by Figures 4-6. Applicant respectfully disagrees. Applicant is unable to find anything in Arrow to support the inference that a management function is linked with the VPN unit using the VPN. As discussed above in connection with claim 11, the management function would be unable to communicate with VPN units to establish a VPN before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 23, the Examiner asserts that Arrow discloses the means for managing the network device using a secure in-band management configuration as the encryption disclosed in column 7. Applicant respectfully disagrees. Nothing in column 7 discloses that the VPN Management Station 160 is a member of any VPN nor that management traffic is encrypted or sent over a VPN.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Per claim 24, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 25, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 26, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 27, the Examiner asserts that the "means+function" claims parallel claims 11-15 and that the claimed elements are met by configuring VPN unit 115 by station 160 to support a VPN, with means linking the management device 160 and its functionality to the VPN via port 908. Applicant respectfully disagrees. Applicant is unable to find anything in Arrow to support the inference that a management device and its function are linked with the VPN. As discussed above in connection with claim 11, the management device would be unable to communicate with VPN units to establish a VPN before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 28, the Examiner asserts that Arrow discloses means for carrying management traffic for the network device using the VPN. As discussed above in connection with claim 11, the management device would be unable to communicate with VPN units to establish a VPN

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 29, the Examiner asserts that Arrow discloses means for managing the network device using the management traffic carried on the VPN. As discussed above in connection with claim 11, the network device could not be managed to establish a VPN using VPN carried management traffic before the first VPN is established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Per claim 30, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 31, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claims 32-41, claims are made to a machine-readable medium to carry out the method as claimed in claims 1-5 and 11-15. The rejections of claims 32-41 are traversed on the same basis as the traversal of claims 1-5 and 11-15 set forth above.

Per claim 42, applicant agrees that the VPN of Arrow is built over a public network, as are most VPNs. Applicant disagrees that Arrow discloses that the management station sends management traffic over a VPN for the reasons discussed above.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Per claim 43, the Examiner asserts that Arrow discloses the management traffic using secure in-band management due to the use of at least the encryption of column 7. Applicant respectfully disagrees. Nothing in column 7 discloses that the VPN Management Station 160 is a member of any VPN nor that management traffic is encrypted or sent over a VPN.

Per claim 44, the Examiner asserts that Arrow discloses a one or more management port 414 is linked with the VPN for management thereof. Applicant respectfully disagrees. Arrow discloses that a VPN unit forward or discard traffic is not being passed between members of the same VPN. Col. 7, lines 26-45. Thus Arrow clearly shows that the network communication port 414 is not limited to VPN traffic and nothing in Arrow discloses that the communication between the management station and the VPN unit, which is not traffic being routed through the VPN unit, is carried on a VPN.

Per claim 45, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Per claim 46, applicant relies on the patentability of the claims from which this claim depends to traverse the rejection without prejudice to any further basis for patentability of this claim based on the additional elements recited.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-5, 11-15, 16-21, 22-31, 32-41, and 42-46 under 35 U.S.C. § 102(e) as being anticipated by Arrow.

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

Rejection Under 35 U.S.C. § 103

5. The Examiner rejects claims 6-10 under 35 U.S.C. § 103(a) as being unpatentable over Arrow et al. (6,175,917) in view of applicant's admitted prior art (APA).

The Examiner asserts that Arrow sets forth a substantial portion of the claimed subject matter via the anticipation analysis such as applied to claims 1-5. The Examiner refers to Figure 4 of applicant's specification which shows a prior art router that includes a plurality of VPN input/output links at 422A-C. The Examiner asserts that it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify a VPN unit 115 per the teachings of the APA Figure 4 so that it is possible to facilitate private communications on the particular router or the same modules on other routers.

Applicant respectfully disagrees that there is any suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings in the way suggested by the Examiner. Arrow teaches a system that provides a virtual private network operating over a public data network. There is no motivation to combine the teachings of APA with Arrow because the combination would not provide anything not already provided by the teachings of Arrow.

Second, applicant submits that there is no reasonable expectation of success in the proposed combination. Arrow teaches a system for loading an operating system in a VPN unit connected to a public network through commands and configuration information transmitted through the public network. Col. 6, lines 31-34. The proposed combination would transmit commands and configuration information over a VPN. However those commands and

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

configuration information include information required to configure the VPN unit to establish VPNs including the first VPN. Col. 9, lines 33-46. If the VPN unit receives management traffic from the VPN, that traffic can hardly be used to provide information required to configure the first VPN unit and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Finally, the prior art references when combined do not teach or suggest all the claim limitations. Neither Arrow nor APA, singly or in combination, teach or suggest a routing and forwarding module to receive management traffic over the VPN. Arrow instead teaches away from receiving management traffic over the VPN because the Management Station provides commands for establishing a virtual private network that operates over a public network. If the VPN Management Station 160 is used to establish a virtual private network, the VPN Units 115 cannot receive management traffic over the VPN to establish the first VPN using the VPN that is not yet established and nothing is disclosed to indicate the configuration of the first VPN is handled specially.

Further, neither Arrow nor APA, singly or in combination, teach or suggest a management module to receive the management traffic over the VPN. Arrow does not show a management module. APA shows a management module 410 connected to receive management traffic over the non-secure data links such as the core data links 420. Specification, page 4. The internal management connection 411 between the management module 410 and the generic routing and forwarding module 412 shown in APA is in great contrast to the inventive internal management VPN link 711 between the management module 610 and the management VPN

Appl. No. 09/738,807
Amdt. dated 01/20/2005
Reply to Office Action of 10/21/2004

module 655 shown in Figure 7. The external management VPN links 624 of Figure 6 are likewise distinct from the disclosure of APA.

The rejections of claims 7-10 are further traversed on the same basis as claims 2-5 discussed above.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 6-10 under 35 U.S.C. § 103(a) as being unpatentable over Arrow in view of APA.

Conclusion

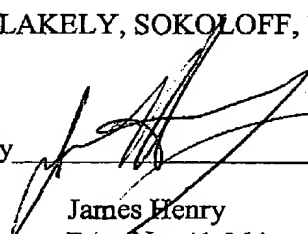
Applicant respectfully requests that a timely Notice of Allowance be issued in this case. The Examiner and the applicant currently have a very different understanding of Arrow. If the Examiner's understanding of Arrow is unchanged after consideration of the above remarks, the Examiner is invited to initiate a telephonic interview with the undersigned with a view toward advancing the prosecution of this application before preparing an Office Action that merely restates the Examiner's position.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 01/20/2005

By


James Henry
Reg. No. 41,064
Tel.: (714) 557-3800 (Pacific Coast)